جامعة نايف العربية للعلوم الأمنية

Naif Arab University For Security Sciences

جرائم الاحتيال بالبطاقات الائتمانية وأساليب مكافحتها

أ. رياض فتح الله بصلة

٢٠٠٢م

جرائم الاحتيال بالبطاقات الائتمانية
وأساليب مكافحتها

أ. رياض فتح الله بصلة

جرائم الاحتيال بالبطاقات
الائتمانية وأساليب مكافحتها

المقدمة

وجدت بطاقة الائتمان نتيجة لتغيير نوعي في عمليات الدفع ونتيجة لأسباب موضوعية فقد ارتبط التحول العالمي من المستندات والوثائق الورقية إلى المستندات والوثائق اللدائنية بمحاولات البحث عن حل مناسب للتكاليف الباهظة لمعالجة المعلومات الضخمة في الصناعة المصرفية ، ففي أمريكا مثلا تتم كتابة حوالي ٤٠ بليون شيك في السنة ويصل تكاليف معالجتها الى حوالي ٣٠ بليون دولار سنويا ، كما يعتبر التعامل بالنقد الورقي أكثر كلفة للمصارف والحكومة[١] . ومع تحول المصارف إلى استعمال الحواسيب لحفظ تسلسل الأحداث في حسابات العملاء وأسواق النقد العالمية ظهرت الوسائل الالكترونية لتحل محل النقد وأوامر الصرف (الشيكات) لكي يسهل تحويل النقود من حساب لآخر [٢] وهكذا بدأت تحل بطاقات الائتمان اللدائنية محل النقد والشيكات ، ويقدر الخبراء عدد البطاقات المستخدمة في أمريكا وحدها بألف مليون بطاقة ممغنطة في التداول[٣] وقد أقبلت على تداولها شعوب أمريكا وأوروبا حتى صارت صناعة بطاقة الائتمان صناعة تنافسية [٤] كونها مناسبة للدفع والمحاسبة الفورية [٥] كما أنها رخصية ويمكن التعامل بها عالمياً وعلى مدار الساعة ، وهي ذات ائتمان قصير المدى على المشتروات وذات دين محدود ومسئولية قانونية محدود في حالة ما إذا تعرضت البطاقة للفقد أو السرقة [٤] وفي مصر لوحظ زيادة مستمرة في الشراء بالبطاقة (لطفا أنظر التحليل الاحصائي للتعامل ببطاقة الائتمان في مصر بيان رقم (١) .

ومع نمو صناعة وتداول بطاقة الائتمان عالمياً ، صاحب ذلك نمو في التلاعب والتحايل بها وإذا صدق الخبر الذي نشرته مجلة الاقتصادي في عددها الصادر في ٣٠ نوفمبر ١٩٩٣م [٦] من أن هناك ستة آلاف مؤسسة تقوم باصدار بطاقات ائتمان في أمريكا ، فإنها لا بد مهزلة تعكس انفراط عقد الحرية وفوضى اقتتصادية تفسر ضخامة الخسارة الناتجة عن التحايل ببطاقة الائتمان [٧] ونظرة سريعة على الإحصائيات التي رصدت الخسارة الناتجة عن التلاعب والتحايل بالبطاقة لصارت هناك ضرورة عالمية ومحلية لوضع ضوابط أمنية واقتصادية وتشريعية على عمليات إصدار بطاقة الائتمان [٧] فقد بلغت الخسارة في سنة ١٩٨٧م مائة مليون دولار أمريكي ، وفي سنة ١٩٩١م بلغت الخسارة ٣٥٠ مليون دولار أمريكي ، وفي سنة ١٩٩٢م بلغت الخسارة ٨٦٤ مليون دولار أمريكي ، أما في سنة ١٩٩٣م فان الخبراء يتوقعون أن تصل الخسارة الى بليون دولار أمريكي [٨] وتؤكد بعض الدراسات الأمريكية والكندية [٤، ٩] على وجود جماعات نيجيرية وجاميكية منظمة ونشطة في تزييف بطاقات الائتمان على نطاق واسع ، كما تشير هذه الدراسات الى الأنشطة الماهرة لجماعات الجريمة المنظمة في الشرق الأقصى في تزييف بطاقات الائتمان ، وقد وجد أن حوالي ٩٠٪ من القضايا ترتبط بأفراد ذوي جذورآسيويه ذات قدرة عالية على الحركة والسفر عبر الحدود لذا كان ارتفاع استخدام البطاقات الائتمانية في مصر بشكل كبير بناء على هذه البيانات الآحصائية للاستخدام والآتي بيانها :

ـ زيادة استخدام بطاقات الدفع بنسبة ٧٥٪ سنة ١٩٩٩م عن عام ١٩٩٨م ليصل إلى ١,٣٤٠٨٠٦ دولار أمريكي .

ـ زيادة عدد بطاقات الدفع إلى ٢٩٠ بطاقة بزيادة ٣٣٪ من احصائيات ديسمبر١٩٩٨م.

ـ زيادة عدد التجارالذين يقبلون تسوية مدفوعاتهم بطاقات الدفع الى ١٥٧٠٠ تاجر.

ـ عدد ما كينات السحب الآلى ٧٦٣ ماكينة على مستوى الجمهورية .

ـ عدد نقاط البيع الالكتروني طرف التجار تصل ٥٧٠٠ .

ـ عدد البنوك الأعضاء في جمهورية مصر العربية ٢١ بنكاً.

ـ عدد الحركات التي تتم داخل مصر باستخدام البطاقات ٥٦٩٠٠٠ حركة سنوياً والمبالغ التي استخدمها الأجانب داخل مصر لشراء سلع أو خدمات يصل إلى ٥٧٥٤٦٦٨٠٠ دولار.

بيان احصائي بعدد القضايا المضبوطة لجرائم بطاقة الائتمان بجمهورية مصر العربية خلال الفترة ١٩٩٤ ـ ١٠/ ١٩٩٨م

السـنة	مزورة	صحيحة بموجب مستندات مزورة	تزوير الاشعارات	الإجمالي
١٩٩٤	٢	٣	ـ	٥
١٩٩٥	ـ	١	ـ	١
١٩٩٦	٥	٤	٥	١٤
١٩٩٧	٦	٤	٢	١٢
١٩٩٨	٣	٣	١	٧

جملة المبالغ المستولى عليها	
المبالغ بالجنية المصري	٦٣٣,٢٠١
المبالغ بالدولارات الأمريكي	٥٧,٠٣١
المبالغ بالريال السعودي	٣٠٠,٠٠٠

يبدو بعض الجماعات ضعيف التنظيم والبعض الآخر على درجة عالية من الكفاءة والتنظيم في تنفيذ مخططاتهم وعملياتهم ، البعض الأول يذهب الى منطقة معينة ثم يشتري بضائع على قدر استطاعته مستخدما في ذلك البطاقات المزيفة ثم يرحل هرباً ، أما البعض الآخر فانه يقوم بانتاج البطاقات المزيفة في دولة عن طريق الاستحصال على معلومات صحيحه من مكان أو أماكن مختلفة من العالم ، وإرسال هذه البطاقات المزيفة للتداول في مكان ثالث من العالم واستخدامها في أغراض غير شرعية[٤، ٩] وتشير بعض التقارير المحلية [١٠-١٤] الى حالات السرقة والتحايل ببطاقة الائتمان في السوق العربية، فقد خسر السوق الأردني ما قيمته ٥٢ ألف دولار أمريكي في ١٩٩٤م وجرى ضبط ٣٥ بطاقة مزيفة يحملها سواح أجانب .

أما السوق المصري فقد خسر حوالي ٣٠٠ الف دولار أمريكي في ١٩٩٣م ، كما جرى ضبط ٢٣ بطاقة ائتمان مزيفة في السوق الأماراتي يحملها أجانب في سبتمبر ١٩٩٤م ، وبالرغم مما تشير إليه تقارير أخرى إلى أن الخسارة الناتجة عن التحايل ببطاقة الائتمان أقل من واحد في الألف من جملة المباع ، إلا أن الحوادث تدل على أن التحايل يزداد بنسبة ١٥٪[١٥] بيان رقم (٣)

ويصنف البعض من علماء علم الجريمة ورجالات البحث الجنائي

جرائم بطاقة الائتمان على أنها أحد اشكال السرقة أو اللصوصية (Larceny Offenses)[١٥، ١٦] مثلها في ذلك مثل أساليب التحايل بالشيكات، على إننا نرى أنها جريمة ذات خصوصية تستوجب أساليب ورؤية وبحثاً وتحريات مختلفة ولا مناص أمام الخبراء وضباط المكافحة وجهات التحقيق والتشريع إلا الاستعداد للخطوة القادمة : عمله بلاستيكية بتقنيات جديدة ومجرم جديد ومفاهيم جديدة للجريمة ومسرح لها يسع العالم كله ، الأمر الذي يتطلب أساليب جديدة وفكراً ومنطقاً وثقافة مختلفة في البحث والفحص، وأعماقاً جديدة في مسارات التحري والضبطية والتحقيق ، ونصوصاً قانونية وتشريعية تضبط كل هذا وتتهيأ له[٧] .

على أن نقطة البدء عندنا هي دراسة البطاقة من حيث هي نظام والوقوف على مسارات الدفع بها ومسارات التحقق والتفويض بواسطتها، ولما كانت الوظيفة الأساسية للبطاقة هي الدفع، ولما كانت المكونات المادية والمعلوماتية للبطاقة تحدد في النهاية استخداماتها ونظام الدفع بها، فان دراسة العلاقة بين نظم الدفع ونظم التكوين جديرة بالفحص والتحليل والتمحيص في محاولة لبيان كيف تستغل بواسطة المجرم في التحايل والتلاعب بالبطاقة وبيان ما تحمله من مسارات الدفع بها من مخاطر كامنة، وبالرغم من أهمية زاوية النظر هذه إلا أنها لم تلق انتباها سابقاً من الباحثين .

على أن الباحث في بطاقة الائتمان سوف يلاحظ أن العلاقة وطيدة بين المكونات المادية والمعلوماتية للبطاقة ومسارات الدفع بها من ناحية ، وبين الجرائم وأساليب التحايل بالبطاقة من ناحية أخرى، مثال لذلك تزييف البطاقة واستبدال الشريط الممغنط وإمكانية استنساخ ما عليه من بيانات وإمكانية تنشيط قيم الدفع المخزنة به، وتعني جميعها أن الدفع بالبطاقة الممغنطة يعتمد اعتماداً رئيساً على الشريط الممغنط .

من حيث هو أداة ادخال وتخزين وتأمين ومكون من مكونات البطاقة ومحدودية تأمينه ، كما أن التحقق من صلاحية البطاقة يعتمد الى حد كبير على موظف البيع في المحلات والمتاجر والمؤسسات التي تقبل التعامل بالبطاقة ، هناك اذن مخاطر كامنه مردها مكونات البطاقة ومسارات الدفع بها .

لذلك جرى هيكلة هذا البحث كي يتناول المبحث الأول مفهوم جرائم التزييف والتزوير وما جري عليه من تحورات نتيجة للتحولات العالمية الراهنة في مسار جرائم التزييف والتزوير ، وينقلنا ذلك إلى المبحث الثاني الذي يناقش عمليات الدفع والتسوق ببطاقة الائتمان من واقع تجربة فعلية أجريناها في حدود دولة قطر أو انطلاقا منها ، ومن شأن ذلك أن يؤدى إلى المبحث الثالث نفصل فيه طرق وأساليب التحايل ببطاقة الائتمان .

مفهوم جرائم التزييف والتزوير

ارتبط مفهوم التزييف بجرائم العملة بينما ارتبط مفهوم التزوير بجرائم المحررات والمستندات من غير العملة ، ويفرق الخبراء بين أسلوبين من أساليب التزييف هما التزييف الكلي والتزييف الجزئي[١٧] ولا غيره هنا عما إذا كانت العملة معدنية أو ورقية ويقصد بالتزييف الكلي هو محاكاة العملية الصحيحة بداية لنهاية عن طريق اصطناع عمله غير حقيقية أو غير صحيحيه ، حيث يقوم المزيف بمحاكاة كاملة لكافة مكونات العمله الصحيحة أو لمعظمها ، أما التزييف الجزئي فيقصد به التغيير في بعض الخواص الظاهرية لعمله صحيحه عن طريق التعديل أو المحو أو الإضافة أو كل هذا أو بعضه أو غيره[١٧-١٩] . وقد خصص القانون المصري مصطلح التزييف ليصف أفعال الانتقاض أو التمويه في العمله المعدنية دون العمله الورقية ، أما ما يطلق

عليه الخبراء تزييفا كليا فقد اصطلح على تسميته بالتقليد وما يطلق عليه الخبراء تزييفا جزئياً فقد اصطلح على تسميته بالتزوير في القانون ، وواضح من نص المادة ٢٠٢ من قانون العقوبات المصري أن التزييف لا يقع إلا على عملة معدنية بينما قد يكون موضوع التقليد عملة معدنية أو عملة ورقية ، كذلك قد يقع التزوير على عملة معدنية أو عملة ورقية ولكن التزوير أكثر وقوعاً وأكثر تصوراً في العملات الورقية .

أما خبراء الولايات المتحدة للخدمات السرية ومن يجري جريانهم في أوروبا وأمريكا فيطلقون مصطلح عملة مقلدة Conuterfeit للدلاله على مايسمونه بالتقليد الكلي (Wholesale imitation) لعمله صحيحه وهو ما يطلق عليه الخبراء العرب التزييف الكلي ، بينما يطلقون مصطلح عمله مزورة (Forged) على العمله الصحيحه التي جري تغييرها (Altered) أو تحويرها(Modified) بطريقة أو بأخرى وهو ما يطلق عليه الخبراء العرب التزييف الجزئي وهم في ذلك لا يفرقون بين كون العمله ورقية أم معدنية ولذلك يقولون عمله ورقية مقلدة (Conuterfeit note) ويقولون عمله معدنية مقلدة (Conuterfeit coin) كذلك يقولون عمله ورقية مزورة (Frged note) ويقولون عمله معدنية مزورة أو تعرضت للتغيير (ALtered or forged coin) وفي هذا البحث يستخدم مصطلح التقليد ليدل على أن التزييف الكلي مرادف له كما يستخدم مصطلح التزوير بدلاً على التزييف الجزئي ومرادف له ويستخدم لفظ التزييف فقط ليدل على المصطلحين معاً وبغض النظر عن كون العملة ورقية أم معدنية أم بلاستيكية .

وقد صاحب تنامي الدفع ببطاقة الائتمان ظهور نمط جديد من الجريمة ونسل جديد من المجرمين وصاحب انتشارها الواسع والتقنية فيها وآليات التأمين بها والخصوصية المميزة لارتكاب الجرائم وأساليب التحايل بها

والنظم التي تعمل في محيطها مجموعة من التحولات ، تركت بصماتها على جرائم التزييف والتزوير سواء في الأساليب والطرق أو في المحتوي والمضمون وهذه التحولات هي :

من الجرائم الورقية الى الجرائم البلاستيكية

ان جرائم تزييف وتزويرالنقود والشيكات والشيكات السياحية هي جرائم ورقية، أما جرائم بطاقات الائتمان فهي جرائم لدائنية أوبلاستيكية أي أن العالم يتحول من الجرائم التي يستخدم فيها الورق كوسيط وأداة للجريمة الى الجرائم البلاستيكية .

كما أن التخوف العالمي من التطورالتقني في اساليب الاستنساخ الملونه عن طريق الناسخات والطابعات الملونه، قد صاحبه الاتجاه نحوأفول دور المستندات الورقية والاتجاه نحو تصاعد دورالمستندات البلاستيكية في الدفع، فالعمله الورقية أوالشيكات التي يمكن أن يجري تزييفها تزييفاً كليا عن طريق التقليد بواسطة الآت النسخ الملونة ـ اذا افترضنا امكانية تداولها والانخداع بها فان ذلك لا ينطبق على بطاقات الائتمان والتي تتميز بآليات تأمينية عديدة ضد الاستنساخ الملون .

من المكونات المادية الى المكونات المعلوماتية : جرائم معلوماتية

إن جانبا عظيما من الجرائم البلاستيكية هي جرائم معلوماتية فالمكونات المادية لبطاقة الائتمان هي في الحقيقة معلوماتية أيضاً مثل لذلك الشريط الممغنط والرقيقه المجهرية والحروف المقرؤة بصرياً، أي انه لا يكفي تقليد جسم البطاقة لكي تتحقق جريمة التزييف بها كما هو الحال في تزييف العملات الورقية والشيكات بأنواعها .

ذلك ان جانباً من تأمين بطاقة الائتمان لاينصب فحسب على تأمين البطاقة من حيث هي مكونات مادية لمنع تزييفها ، بل يجب أن ينصب التأمين كذلك على حماية المكونات المعلوماتية للبطاقة .

في تزييف العملات والشيكات الورقية يكفي أن يتقن المزيف تقليد المكونات المادية لها كي يستخدم العملة أوالشيك بعد ذلك في التداول ، أما في حالة بطاقات الائتمان فان انتاج بطاقة ائتمان مقلدة على درجة عالية من التقليد لايكفي وحدة لاستخدام البطاقة في التداول والدفع إذ أن هناك مرحلة أكثر أهمية وهي تقليد المكونات المعلوماتية للبطاقة توطئة لاستخدامها في الدفع والتداول .

لذلك ففي عصر المعلومات وعصر النقود الالكترونية لا يكفي التقليد المادي للبطاقة لوقوع فعل التزييف المجرم بالقانون إذ أن الاستحصال على المعلومات الخاصة بالبطاقة لا يقل أهمية عن تقليد البطاقة مادياً وهو ما يعني أن تقليد بطاقة الائتمان يتطلب تجهيزات مادية وتجميعات معلوماتية .

من التزييف المحلي إلى تزييف عالمي التأثير

ان تقليد بطاقة الائتمان يمثل تهديداً مباشراً وفورياً وسريعاً للاقتصاد العالمي والمحلي وحقوق الأفراد بغض النظر عن موقعهم في العالم أي أنه يمكن القول أن تقليد العملات الورقية والشيكات يمثل تهديداً موضعياً محدوداً يمكن التحكم فيه ، أما تقليد بطاقة الائتمان فانه يمثل تهديداً سرطانياً يتأثربه حامل البطاقة في أي موقع من العالم . وقد نبه مؤتمر الانتربول الثامن المنعقد في أتاوا بكندا في ١٩٩٢م إلى تعاظم مخاطر جريمة بطاقة الائتمان والى عالميتها حيث يتم اعداد وتصنيع البطاقات المزيفة أوالمزورة في دولة بينما تجمع المعلومات اللازمة عن بطاقة الائتمان الصحيحة من دولة إلى

دول أخرى ويجري ترويج البطاقات المزيفة في مكان ثالث من العالم، ذلك أن التقنية الحديثة كالفاكس ووسائل الاتصال المتقدمةوالمعلومات الائتمانية الآلية المنتشرة عالمياً قد أتاحت جميعها للمزيف فرصة سلب حقوق الآخرين في أي مكان من العالم هذا من ناحية ثانية فهناك أدلة قوية على أن معظم جرائم بطاقة الائتمان التي وجدت صداها في أمريكا وكندا واستراليا واسبانيا وغيرها ذات علاقة بجماعات المنظمة في الشرق الأقصى خاصة في هونج كونج.

ما الذي يعنيه كل هذا؟

أولاً: يعني أهمية التعاون الدولي والأقليمي في قضايا وجرائم الائتمان بغرض تبادل المعلومات عن طريق إنشاء مكاتب دولية وأقليمية والدعوة إلى إنشاء قسم خاص داخل إدارات مكافحة التزييف والتزوير بوازارت الداخلية العربية يكون متخصصاً في جرائم بطاقة الائتمان، وتدريب العاملين به على أساليب التحري والضبطية في هذا النوع المميز من القضايا.

ثانياً: إنشاء قاعدة بيانات تتضمن معلومات كافية عن قضايا بطاقة الائتمان سواء في الداخل أو الخارج وأهم الخواص التي تميزأنواع البطاقات التي جرى تزييفها أو تزويرها وأماكنها وتاريخها وأسماء المتهمين فيها للاستعانة بها في عمليات الربط وتحديد المصدرعالمياً وإقليمياً.

تحليل عمليتي الدفع والتسوق ببطاقة الائتمان

أجريت عملية اختيار ميدانية محدودة للتعرف على استخدام بطاقة فيزا البنك العربي في الدفع والتسوق في حدود دولة قطرأوانطلاقاً منها

وذلك في محاولة للوقوف على مسارات الدفع بالبطاقة، وكيف يمكن التحايل من خلال هذه المسارات وتم اختيارثمانية مواقع بحيث تسمح بالتنوع في طرق الدفع ومدى الاحتياج لإدخال رقم الهوية الشخصي ـ يسمي أيضاً الرقم السري (Personal Identificaion number [PIN]) وسجلت النتائج في الجدول المرفق وبالرغم من محدودية هذا الاختيارإلا أنه يلقي بعض الضوء على مسارات الدفع ببطاقة الائتمان ، وقد لوحظ أن صورة العميل على البطاقة لم تتعرض للتدقيق من قبل موظف البيع ولعل السبب في ذلك مرده ندرة البطاقات المزودة بصورة العميل في الوقت الراهن ، كما يتضح عدم طلب ادخال الرقم السري إلا في حالة سحب مبالغ مالية بواسطة ماكينة الصراف الآلى وفي المرات التي تم فيها مضاهاة توقيع العميل على البطاقة بتوقيعه على فاتورة الشراء فان عملية المضاهاة تتم بسرعة ، وتكاد تنحصرعملية التحقق من بيانات البطاقة في معرفة تاريخ انتهاء صلاحيتها وأنه كلما كان عدد رواد المتجر كثيفا كلما قلت فرص التحقق من توقيع العميل وبيانات البطاقة وإذا كان العميل معروفاً لموظف البيع فان هذا الأخير عادة لا يتحقق من توقيع أوبيانات العميل وقد لوحظ كذلك أن هناك ثقة مسبقة في الدفع ببطاقة الائتمان عند موظفي المتاجر التي تقبل التعامل بهذه البطاقات .

الدفع المعتمد على بيانات الشريط الممغنط (التحويل بواسطة مطراف)

يتم الدفع حسب الخطوات الآتية :

١ ـ يضغط الموظف على مفتاح الدخول في لوحة المفاتيح ، فيظهراسم المتجر على شاشة المطراف عمرافندي مثلاً .

٢ ـ يدخل الموظف البطاقة في مجرى خاص بالمطراف ، ساحباً أياها بسرعة نسبية وذلك لقراءة المسجل على الشريط الممغنط .

٣ ـ إذا قبل النظام البطاقة ، يظهرعلى الشاشة عبارة أدخل الكمية ، أي قيمة المبلغ المشترى به .

٤ ـ يقوم الموظف بالضغط على مفتاح الدخول ويدخل ثمن المشتريات أي المبلغ أوالكمية .

٥ ـ يظهر على الشاشة ما يفيد الانتظار ، حيث يتصل المطراف بالحاسب المركزي أوحاسب الشبكة لمعالجة عملية البيع والشراء .

٦ ـ فإذا كان سقف البطاقة أوحساب العميل يغطي عملية الشراء ، يظهر على شاشة المطراف عبارة نقوم بطباعة الفاتورة .

٧ ـ يخرج من المطراف فاتورة المعاملة من أصل وصورة ، في الوقت الذي يظهرفيه على الشاشة رقم العملية أورقم التفويض Authorized code .

٨ ـ يقوم الموظف بأخذ الفاتورة من المطراف ، ويطلب من العميل توقيع الفاتورة بخط اليد فتطبع صورة للتوقيع بصورة الفاتورة .

٩ ـ عندئذ يقوم الموظف بالتحقق من رقم البطاقة وتاريخ انتهاء صلاحيتها وهي ذات الأرقام والبيانات التي تظهر بفاتورة الحساب ، كما يقوم بالتحقق من صحة التوقيع ، ويعطى الصورة للعميل ويحتفظ بالأصل ، وتنتهي العملية .

اختيار ميداني

لمسارات الدفع وسحب نقدية بواسطة بطاقة فيزا البنك العربي

البطاقة	الموقع	عدد الزيارات	كثافة العملاء	طريقة القيد أو التحويل	الرقم السري	مضاهاة التوقيع	مقارنة البيانات	الصورة
فيزا البنك العربي وهي بطاقة دفع مؤجل مزودة بصورة ملونة للعميل على ظهر البطاقة	عمر أفندي قطر	٢	قليلة	مطراف	لم يطلب	تم	تم	لم تلاحظ
	الركن الرياضي	٢	متوسطة	مطراف	لم يطلب	تم	تم	لم تلاحظ
	سوق الدوحة المركزي	٢	كثيفة	مطراف	لم يطلب	لم يتم	لم يتم	لم تلاحظ
	بيتزاهت الكورنيش	٢	كثيفة	مطراف	لم يطلب	تم	تم	لم تلاحظ
	في طائرة طيران الخليج	٢	قليلة	ختامة	ـ	تم	تم	لم تلاحظ
	المكتبة المثالية	٣	قليلة	ختامة	ـ	لم يتم	تم	لوحظت
	الصرف الآلي	٥	ـ	مطراف	طلب	ـ	ـ	ـ
	بالمراسلة لدورنشر أوروبية وأمريكية	٣	ـ	٣	ـ	أتمت	أتمت	ـ

تبدأ المعاملة بقراءة البيانات على الشريط الممغنط بواسطة مطراف، وتهدف هذه الخطوة إلى التعرف على البطاقة وربما أيضاً التعرف على ما إذا كانت صحيحة من عدمه، حيث تسمح البيانات الموجودة على الشريط الممغنط ـ وهي في الغالب رقم البطاقة وتاريخ انتهاء صلاحيتها ـ إلى حث الحاسب في البنك لاستخراج البيانات الخاصة بالتعرف على البطاقة ـ وليس حامل البطاقة ـ وذلك من خلال قاعدة البيانات البنكية، أي يتم التعرف على البطاقة، ورقم حساب الشخص المصدرة له البطاقة، والبنك المصدر للبطاقة، ونوع البطاقة، وغير ذلك من البيانات التي يحتاجها الحاسب لمعالجة عملية البيع والشراء، وإذا كانت البطاقة بطاقة تحويل إلكتروني عند نقاط البيع، فإنه يتم حسم المبلغ من حساب العميل واضافته إلى حساب التاجر، حيث أن البرامج المستخدمة تسمح أيضاً بتعرف الحاسب على المطراف ونقطة البيع التي يتم عندها الشراء.

أما التحقق من شخصية حامل البطاقة من قبل موظف البيع فإنه يتم على مرحلتين، الأولى تتضمن التحقق من رقم البطاقة وتاريخ انتهاء صلاحيتها على البطاقة وعلى فاتورة الحساب، والثانية تتضمن مضاهاة توقيع العميل على البطاقة بتوقيعه على فاتورة الحساب أمام الموظف، ويعتبر إدخال العميل لرقم الهوية الشخص أو الرقم السري أحد أساليب التحقق من شخصية حامل البطاقة والتي يقوم بها الحاسب، ولكن هذه الخطوة لايتم تطبيقها إلا عند استخدام مطراف الصراف الآلي لصرف مبالغ مالية سائلة، أي أنه عند الشراء أو تلقي الخدمات لا يدخل العميل رقم الهوية الشخصي.

ويتضح من ذلك أنه إذا كانت البطاقة مسروقة، ثم جرى كشط شريط التوقيع، ولصق شريط آخر عليه توقيع لم يتم كتابته بخط يد صاحب البطاقة الأصلي، فإن عملية البيع والشراء والدفع سوف تتم، وسوف يقيد المبلغ

على حساب الشخص الذي صدرت البطاقة باسمه أصلاً، وهذه فجوة في تصميم بطاقة الائتمان وفي مسار الدفع بها.

وإذا كانت البطاقة بطاقة تحويل إلكترونياً عند نقاط البيع فقد تتم المعاملة مباشرة على الخط (On-line) بواسطة الهاتف، أو خارج الخط (Off-line)، والذي تدان فيه المبالغ مع نهاية اليوم، أو الجمع بين الأسلوبين، حيث يتم التأكد من الاعتماد على الخط، وتتم الاستدانة في نهاية اليوم (اقرأ أيضاً تحليلنا للمخاطر الكامنة عند عرضنا لأحدث نظم مطاريف نقطة البيع والشراء وأجهزة ادخال الرقم السري وأجهزة الصراف الآلي حال استخدام بطاقة الائتمان لصرف مبالغ نقدية، في مطالب ثلاثة تالية في مبحثنا الحالي).

الدفع المعتمد على البيانات المقروءة بصرياً

(لا تتضمن عملية التحويل خطوات الإلكترونية)

قد تتم عملية التسويق بالمراسلة حيث يقوم العميل بوضع رقم بطاقة الائتمان، وتاريخ انتهاء صلاحيتها، ثم يكتب المبلغ اللازم، ثم يوقع في موضع التوقيع بالفاتورة أو الايصال، ويرسل الفاتورة بالبريد إلى الجهة المعنية، وهنا تكمن أحد مخاطر طرق استخدام بطاقة الائتمان إذ يكفي أن يعرف المجرم رقم بطاقة شخص وتاريخ انتهاء صلاحيتها، كي يقوم باثباته على الفاتورة، ثم التوقيع باسم صاحب البطاقة، هذا من ناحية، ومن ناحية ثانية فإنه يمكن تتبع المجرم عن طريق العنوان وعن طريق خط اليد.

أحياناً لا يكون المتجر مجهزاً الكترونيا بحيث تكون هناك قناة اتصال بين المتجر والبنك، عندئذ أما أن يقوم التاجر بملء بيانات الفاتورة بخط

اليد، ثم يعطى الفاتورة للعميل لتوقيعها، وأما أن يكون لدى التاجر دامغة (ختامة Imprinter) ـ يتم صرفها بواسطة البنك ـ ويقوم التاجر بأخذ طبعة للبطاقة، حيث تظهر البيانات المنقوشة بحروف وأرقام نافرة، ثم يقوم التاجر باثبات المبالغ بخط اليد، ثم يطلب من العميل التوقيع، ويجري مضاهاة لهذا التوقيع.

وينطبق على عمليات الدفع هذه ما سبق ذكره عن عمليات الدفع المعتمدة على بيانات الشريط الممغنط، ونقصد بذلك امكانية سرقة البطاقة، حيث لا توجد وسيلة ـ هنا ـ لمنع استخدام البطاقة بواسطة طرف غير صاحبها الحقيقي.

ولكن هناك فرصة للتزوير والتحايل بواسطة التاجر نفسه أو موظفيه، حيث يمكن تحميل العميل لأكثر من فاتورة عن مشتريات لم يأخذها [٢١]، استغلالاً لوجود بيانات بطاقة العميل تحت يد التاجر عن طريق الفاتورة الصحيحة التي وقعها، ثم يقوم التاجر بتزوير توقيع العميل بأي من طرق التزوير الممكنة للتوقيعات، ويتم ملء البيانات الخاصة بالبطاقة أما بخط اليد، وأما بأخذ أكثر من طبعة للبطاقة على أكثر من فاتورة، ويقوم العميل بالتوقيع على فاتورة واحدة ـ بملحقاتها ـ عن مشترياته، ثم يقوم التاجر بتقليد أو تزوير توقيع العميل على الفواتير الأخرى التي أخذ عليها طبعة بيانات بطاقة العميل عليها خلسة دون أن يدري، وإذا أدرك العميل أنه جرى تحميله فواتير لم يقم بتوقيعها، فإنه قد يطعن عليها بالتزوير، وهناك امكانية عالية لمعرفة الجاني واثبات حدوث التزوير.

وأيا ما كانت طريقة الدفع والتسوق عند نقاط البيع، فالثابت هو أن التوقيع بخط اليد يؤدي دوراً هاما في التحقق من هوية حامل البطاقة أمام

الموظف قد لا يكون مؤهلاً بدرجة كافية للتحقق من سلامة التوقيع من عدمه، وتلك فجوة في نظم الدفع ببطاقة الائتمان، لذلك فإن اضافة صورة العميل لمكونات البطاقة يبدو حلا فعالاً ضد بعض عمليات التحايل بالبطاقة.

مطراف التحويل الالكتروني عند نقطة الخروج

(Pos Transaction Terminal)

يسمح هذا الجهاز بالتحقق من قبول النظام لبطاقة الائتمان وبطاقة الدفع الفوري، ومعد للاستخدام عند مخارج نقاط البيع والشراء، وبواسطة هذا الجهاز يتم التخاطب وتبادل الاجابة بين المطراف والحاسب، ويتطلب الأمر برامج تشغيل لضبط وتسهيل عمليات التخاطب بين المطراف والحاسب، لذا فإنه مزود بمودم (Modem)، ويمكن أن يظهر على الشاشة حروف حتى ٤٨ حرفاً، ومزود بتسعة وعشرين موضعاً في لوحة التشغيل لتسهيل عمليات البرمجة المستقبلية، كما أنه مزود بذاكرة ١٢٨ كيلوبايت، ويستخدم مع طابعات متعددة (Roll Printers)، ويمكن تركيب جهاز إدخال الرقم السري مع هذا الجهاز، أي أن هذه المطاريف مجهزة مادياً وبرامجياً لقراءة البيانات والتشيفرات على الشريط الممغنط.

والجدير بالذكر أن الأجهزة المزودة بشاشة أفضل من تلك الخالية منها، ومن المهم تحديث المطاريف لاستيعاب التطور في تقنية تأمين بطاقات الائتمان.

ما الذي يجعل عملية تزييف بطاقات الائتمان عملية سهلة؟

هو عدم تطبيق الاختبارات اللازمة على البطاقة حال قيام العملاء بالشراء وعدم ضبط النظام بشكل تكاملي، فالعديد من موظفي المتاجر لا

يقومون بمقارنة البيانات المشفرة بالشريط الممغنط ـ خاصة رقم الحساب وتاريخ انتهاء صلاحية البطاقة ـ بظهر البطاقة بالمعلومات المطبوعة طباعة نافرة في وجه البطاقة، ذلك أن الثابت بالتجربة أن العديد من البطاقات المزيفة لا تتماثل فيها البيانات المشفرة والمعلومات المطبوعة، إذ يجب أن تكون واحدة في البطاقات الصحيحة، ويجب القول أن وحدة البيانات المشفرة والمعلومات المطبوعة لا يعني بالضرورة عدم تزييف البطاقة ولكنها مؤشر يدل على إمكانية كونها صحيحة، هذا من ناحية، ومن ناحية ثانية فإن بعض المتاجر تخلو من المطاريف المزودة بشاشة لأظهار البيانات الملقنة للشريط الممغنط.

أدخل بعض منتجي البطاقات في الشريط الممغنط ما يسمى بالشيفران صعبة النسخ (Hard to copy code)، أو ما يسمى أحياناً بالشفيرات الدائمة (كالعلاقة المائية الممغنطة) في البطاقات المصدرة حديثاً، ولكن في معظم الأحيان لا تكون قارئة البطاقة (Scanner) (أي المطراف) في المتاجر مجهزة لقراءة هذه الشيفرات بدقة أو أن برامج معالجة البطاقة في هذه المطاريف تفشل في قراءة الشيفرة بطريقة صحيحة، وبالتالي يضطر الفاحص للعودة للطريقة القديمة للتحقق من مدى صحة البطاقة اعتماداً على الأسم ورقم الحساب وغير ذلك من البيانات بدلاً من التحقق من الشيفرات صعبة النسخ[٨].

ولذلك فإن الاتجاهات الحديثة لتأمين التعامل بالعملة البلاستيكية تتضمن ادخال الشيفرات الدائمة، ودعوة المتاجر لتطوير مطاريف نقطة الخروج حيث تجهز هذه المطاريف لقراءة الشيفرات الدائمة صعبة النسخ، واستصدار القوانين والتشريعات الرادعة في حالة التفريط في المعلومات الخاصة بالبطاقة عن طريق المتاجر، والتقليل قدر الإمكان من إرسال البطاقة بالبريد.

وهناك بعض الدلائل التي تشير إلى أن الشيفرات الجديدة لم تمنع التزوير بالكشط المعلومات (Skimming)، وهي طريقة من طرق التزييف يقوم فيها المزيف بالحصول على بطاقة صحيحة ونسخ كل بت (Bit) (وحدة) من المعلومات الثابتة على الشريط الممغنط بما في ذلك الشيفرات صعبة النسخ[٨].

أساليب التحقق من صحة البطاقة عند نقطة الخروج :

١ ـ مقارنة البيانات المطبوعة بالبيانات المشفرة التي تظهر على شاشة المطراف، وهي أيضاً البيانات التي تطبع في فاتورة نقطة البيع والخروج بواسطة المطاريف المجهزة لذلك.

٢ ـ بواسطة الشيفرات صعبة النسخ مثل العلامة المائية الممغنطة.

٣ ـ التوقيع.

٤ ـ الصورة.

٥ ـ المقارنة النظرية العينية بواسطة موظف نقطة الخروج.

جهاز إدخال الرقم السري (Denit Card Pin Pad)

يتصل جهاز ادخال رقم الهوية الشخصي مباشرة بمطاريف التعاملات بغرض ادخال (تمرير) آمن للبيانات التعرفية (لبيانات الهوية) التي تتطلب تعاملات بطاقة الدفع الفوري.

وقد تم تصميم هذا الجهاز بحيث يوفر سلسلة من عناصر الأمان التي تمنع أي عملية اقتحام أو تطفل على النظام، ذلك أن رقم الهوية الشخصي يجري تشفيره على جهاز الإدخال (الممر Pin Pad) عند الضرب على لوحة المفاتيح، ومرد هذا التشفير هو النقل المؤمن للمعلومات خلال شبكة

الاتصال، هذا من ناحية، ومن ناحية ثانية فإن الرقم لا يظهر على الشاسة ولكن الذي يظهر هو علامة نجمة.

يقوم هذا الجهاز بتشفير البيانات وفقا للخوارزمية القياسية لتشفير البيانات (Data Encryption Standrad (DES) Algorithm)، ويتطلب الأمر برامج خاصة لادارة مفاتيح (للتحكم في مفاتيح) لوحة التشغيل (لوحة الادخال ـ لوحة المفاتيح).

وهذه الأداة مجهزة بحيث تعمل مع الطرفيات (المطاريف) المناسبة لها، ولا تحتاج لمصدر كهربي خاص بها، كما أنها صغيرة الحجم فيسهل وضعها عند مراكز البيع والشراء ومزودة بعدد ستة عشر مفتاحا تتضمن مفتاح الالغاء لمحو الأرقام الخطأ واعادة ادخال الأرقام الصحيحة، كما أنها مزودة بشاشة يمكنها استيعاب ستة عشر حرفاً، ومزودة بذاكرة روم ٣٢ وذاكرة رام ٨ك.

هناك الآلاف من مطاريف التحويل الالكتروني عند نقاط البيع الأمر الذي مكن لمحاول اختراق النظام أن يسرق واحدة منها، ثم يقوم بدراسة مكوناتها المادية والبرامجية وذلك بغرض ايجاد طريقة لقراءة المفتاح السري لهذا المطراف، ثم استخدام هذا المفتاح السري للحصول على قيم أرقام الهوية الشخصية، وقد يكون من الصعوبة بمكان قراءة المفتاح السري ثم وضع المطراف في موضعه للعمل، ولكن المخترق ليس في حاجة للعمل وفق هذه الطريقة، ذلك أنه يمكنه تسجيل مجاميع أرقام الهوية السرية المشفرة، وغير ذلك من بيانات البطاقة التي يحتاجها، ثم العمل على سرقة المطراف واختراقة وقراءة المفتاح السري، وتستخدم هذه المعلومات لتزييف عدد من البطاقات التي استطاع أن يعرف قيم رقم الهوية الشخصي الخاص بها، وبهذه البطاقات المزيفة ـ الحاملة لمعلومات صحيحة ومعلوم رقم الهوية

الشخصي لها ـ يمكن للمخترق استخدام آلات الصراف الآلي وشراء البضائع التي يبتغيها من المحلات والمتاجر المختلفة، ويسمى هذا الاختراق التعقب غير المباشر أو التعقب في الاتجاه العكسي (Backwards Tracking)، ولكن هناك نوعاً آخر من الاختراق هو التعقب أو التسلسل المباشر (Forward Tracking) حيث يستخدم المفتاح السري الذي جرى اكتشافه في الاستمرار في فك شفيرات قيم رقم الهوية الشخصي، ولكن هذا يستلزم أن يستمر استخدام المطراف في العمل عند نقاط البيع بعد استخلاص الرقم السري الخاص به، ومن الواضح أن هذا النوع من الاختراق أكثر صعوبة، وبعض برامج مطاريف التحويل الالكتروني عند نقاط البيع غير مجهزة لمقاومة هذا النوع من الاختراق [٢٢]، والفكرة المحورية التي يعتمد عليها المخترق في الحالتين هي حساب كيف يعالج المطراق أرقام الهوية الشخصية وتشفيرها، وهذا هو المقصود بالمفتاح السري للمطاريف.

ولاحباط هذين النوعين من الاختراق جرى اقتراح مدخلين :

المدخل الأول : يعتمد على تغيير المفتاح السري لكل معاملة (Changing the key for every transaction).

المدخل الثاني، يعتمد على التشفير بالمفتاح العام (Public Key Cryptography) والمطراف الذي عرضنا له هنا يقوم على برامجية المدخل الأول أي يعتمد على تغيير المفتاح السري لكل معاملة، ولذلك يطلق على مفتاح التشفير هنا مفتاح المعاملة (Transaction Key).

ويجب أن نذكر هنا أن هناك تقارير مؤكدة على امكانية اختراق الخوارزمية القياسية لتشفير البيانات (DES) واسعة الاستخدام في أجهزة الصراف الآلي وأجهزة مطاريف الخروج، وأجهزة ادخال الرقم السري [٢٣]،

ولذلك تتجه الشركات المنتجة لهذه الأجهزة إلى اعتماد خوارزمية المفتاح العام والتي تسمى أيضاً (RSA) وهي الحروف الأولى من ألقاب العلماء الذين اخترعوا سنة ١٩٧٧م، وهم (Rivest & Shamir & Adleman)، والجدير بالذكر أن خوارزمية المفتاح العام تسمح بانشاء مباشر للتوقيعات الرقمية (Digital Signatures)، والتوقيع الرقمي هو عدد (Number) يذيل رسالة الشفرة لحل مشكلة التحقق والثبوتية (٣٤ ، ٣٥)، لكن المدهش أن تقارير جديدة قد أثبتت امكانية اختراقها[٢٦]، بالرغم من الدعاية التي صاحبت عمليات تطبيقها لتأمين اتصالات نظم بطاقة الائتمان بأنواعها عند الدفع والتسوق من خلال منظومة شبكة الاتصالات العالمية الحاسوبية (Internet).

ويستخلص من هذا جميعه أن هناك ضوابط يجب الأخذ بها قبل تطبيق الدفع بالعملة البلاستيكية أو بطاقات الائتمان وبطاقات الدفع الفوري، إذ يجب أن تعتمد العقيدة التأمينية على التكامل وتأمين كل مراحل النظام بدءً من البطاقة وانتهاءً بالمطاريف التي توجد في المتاجر والمحلات.

صرف مبالغ نقدية بواسطة بطاقة ائتمان عن طريق أجهزة الصراف الآلي (Automated Teller Machines (ATM)

بالرغم من أن الوظيفة الأساسية لبطاقة الائتمان هي الدفع عند التسوق أو شراء البضائع أو الحصول على خدمات، فقدتم التوسع في استخداماتها لاجراء كافة المعاملات المصرفية كالسحب والايداع، والتحويل في أي وقت على مدار الساعة، وبالاضافة إلى ذلك فقد تستخدم كوسيلة لتحقيق الشخصية خاصة عند صرف الشيكات في دول عديدة كأمريكا وكندا وأوروبا.

في كل نظم أجهزة الصراف الآلي سواء كانت تعمل على الخط، أو

خارج الخط، يعتمد تأمين النظام على كل من البطاقة (مفتاح الدخول) ورقم الهوية الشخصي (المعلومات الضابطة والمتكاملة)، ذلك أنه يمكن ادخال أي بطاقة ممغنطة في الماكينة، لكن محاولات اكتشاف رقم الهوية الشخصي عن طريق المحاولة والخطأ (By trial and Error) يتم احباطها عن طريق البرامج الملقنة للمكانية.

نقطة الضعف الأساسية في النظام كله هو العميل غير المهتم بتأمين رقم هويته الشخصي، كذلك يمكن معرفة رقم الهوية الشخصي عن طريق ملاحظة العميل حال ضغطه على مفتاح الماكينة أثناء اجراء المعاملة، ويأتي بعد ذلك الخطوة التالية وهي الحصول على البطاقة، وما أن تتوفر البطاقة ويتوفر رقم الهوية حتى تصبح عملية سحب الأموال السائلة من الماكينة عملية سهلة، ولكن المردود المالي لن يكون كبيراً، ذلك أنه في كل نظم أجهزة الصراف الآلي يوجد حد أعلى يمكن سحبه في اليوم الواحد ولا يمكن تجاوزه، ولكن المشكلة الحقيقية تبدأ عند استخدام الماكينات خارج الخط، إذ يمكن عن طريق استخدام نسخ عديدة من البطاقة الحصول على أعلى سحب ممكن من الأموال السائلة من عديد من الماكينات التي تعمل خارج الخط، بعبارة أخرى يقوم المزيف بعمل نسخ متعددة من البطاقة وسحب أعلى قدر من الأموال عن طريق الماكينات التي تعمل خارج الخط والمتناثرة هنا وهناك والسبب في اضطرار المزيف لعمل نسخ متعددة من البطاقة هو أن النظام يسجل على الشريط الممغنط ـ في المسار الثالث ـ المعاملة وتاريخها وغير ذلك من البيانات، ويجب القول أنه يمكن للنظام الذي يعمل على الخط أن يعمل أيضاً خارج الخط، وبالتالي يصعب التفرقة بينهما.

ختامة فواتير الشراء ببطاقة الائتمان
Imprinters Addressogratphs

هناك العديد من نظم ختامات فواتير الشراء بواسطة بطاقة الائتمان، نذكر منها هذا النظام المبسط الذي يعمل بمقبض لضخ (Pump) حبر الختامة لطبع البيانات النافرة بالبطاقة على فاتورة الشراء، وتتكون من وسادة من المطاط (Rubber Feet) عليها قاعدة معدنية، ورأس طابعة (Metal Base and Printerd)، ومقبض (Handel) يتحرك لأعلى وأسفل.

وتستخدم الختامات في حالة الدفع المعتمد على البيانات المقروءة بصرياً، أي أن عملية التحويل لا تتضمن خطوات إلكترونية حيث لا تكون هناك قناة اتصال بين المتجر والبنك، ولا توجد هناك وسيلة حاسمة للتحقق من صلاحية البطاقة إذا كانت مصطنعة أو لمنع استخدام بطاقة صحيحة بواسطة طرف غير صاحبها الحقيقي، وفي حالة اصطناع البطاقة عن طريق التزييف الكلي تعتمد عملية التحقق على موظف البيع وفراسته الشخصية في كشف التزييف من خلال معرفته الدقيقة بمواصفات البطاقة الصحيحة، كما تعتمد كذلك على مدى اتقان العملية التزييفية.

والحالة الثانية أيضاً تعتمد على موظف البيع الذي يقوم بمضاهاة التوقيع على فاتورة الشراء بالتوقيع على البطاقة ومقارنة الصورة بالبطاقة بهيئة العميل، ولكن هناك إمكانية لتزوير التوقيع وتزوير الصورة، ولذلك يجب التحقق من سلامة الصورة وسلامة شريط التوقيع.

وتوجد هنا فرصة للتزوير والتلاعب بالبطاقة بواسطة التاجر أو موظفيه، حيث يمكن تحميل العميل لأكثر من فاتورة عن مشتريات لم يأخذها، حيث يتم أخذ أكثر من طبعة للبطاقة على أكثر من فاتورة، ويقوم

العميل بالتوقيع على فاتورة واحدة عن مشترياته، أما التاجر فإنه يقوم بملء الفواتير الأخرى ثم تقليد توقيع العميل عليها، وإذا ادرك العميل أنه جرى تحميله فواتير لم يقم بتوقيعها فإنه قد يطعن عليها بالتزوير، وهناك امكانية عالية لمعرفة الجاني، ويسترشد في ذلك بالآتي :

١ ـ مضاهاة توقيعات العميل موضوع الطعن على توقيعاته الصحيحة.

٢ ـ مضاهاة الخط أو الخطوط المحرر بها الفواتير على خطوط الموظفين أو التاجر.

٣ ـ أخذ طبعات من الختامات الموجودة بالمحل وبيان مدى امكانية وجود اختلاف بين الطبعات المتتالية للختامة وما قد ينشأ من ازاحات أو تأثر وضوح المعلومات المطبوعة.

٤ ـ مقارنة الاختام والأحبار.

صور التحايل والتلاعب ببطاقة الائتمان

لماذا من مدخل معرفي إلى مدخل تحليلي إلى دراسة لنظم الدفع ببطاقة الائتمان، لماذا اختلفنا مع علماء علم الجريمة في توصيف جريمة بطاقة الائتمان، فرأينا أنها جريمة ذات خصوصية تستوجب رؤية في التحري والتحقيق واشتقاق الدليل بأساليب وطرق جديدة ومبتكرة، نعم ولماذا أنتهجنا منهجية معرفية تحليلية تكاملية في عرضنا لبطاقة الائتمان : نتعرف على النظام ونحلل مساراته وندرك مدى التكامل فيه كي نقف في النهاية على كيفية جريان اختراق النظام؟ وما المخاطر الكامنة في مساراته؟ وكيف يمكن تصميم خطط التحري وبحث اجراءات التحقيق ومداره وكيف يكون؟ كيف أمكن تزييف البطاقة كليا وتقليد الشريط الممغنط ونسخ ما عليه من بيانات مشفرة؟ وكيف جرى محو ما على البطاقة من كتابات مطبوعة طباعة

بارزة وإعادة قولبة البطاقة بأرقام حسابات وبيانات جديدة؟ وكيف صارت بطاقة الائتمان مطمع الأجيال الجديدة من قراصنة الجريمة المنظمة؟ وكيف صارت أرصدة الدول والأفراد نهباً مشاعاً لمجرم متعلم يستند إلى مبادئ بسيطة في علوم الالكترونيات والحاسب وطرق التشغيل والبرمجة؟ وكيف تكون في هونج كنج مثلاً أو في نيجيريا وتسرق شخصاً آمناً في أوروبا، أو كندا، أو أمريكا، أو بلاد العرب؟ تسرق دون أن تلتقي بالضحية ودون أن تدخل بيته، أو تفتح خزانته ودون أن تحمل سلاحاً، انها اذن جريمة السرقة عن بعد، ففي عالم الريموت كنترول يأتي النهب بالريموت ودون كنترول إذا صح التعبير.

نحن الآن أمام ثلاثة عناصر كل منها يمثل ضلعاً من مثلث متساوي الأضلاع، الضلع الأول هو البطاقة، والضلع الثاني هو المعلومات، والضلع الثالث هو النظام، ومن هذه العناصر الثلاثة يتكون النظام الكلي لبطاقة الائتمان ولا عبرة هنا عما إذا كانت البطاقة ممغنطة أم رقائقية، أم بصرية، هذه العناصر متكاملة متآزرة في صورتها الافتراضية النموذجية، وانها كالجسد الواحد، أنظر مثلاً إلى تجهيز مطاريف الصراف الآلي كي تقبل فقط استخدام علب السجائر، أو أي مكون بأبعاد البطاقة والتي يمكن ادخالها في الفتحة الخاصة بقارئة البطاقات بالمطراف، وينجز ذلك عن طريق تزويد أجهزة الصراف الآلي بغطاء متحرك وبنظام للتعرف على البطاقة (Card Detection System)، والذي يسمح فقط للبطاقة الممغنطة بالدخول في الجهاز، ويتعرف على ما سبق أن أطلقنا عليه نظام التعرف على أبعاد البطاقة وبالتحديد على عرض البطاقة، وكذا يتعرف على البيانات المشفرة بطريقة ممغنطة على البطاقة، هذا المسار قد يمنع عمليات التخريب العرضية، ولكن استخدام البطاقة الممغنطة في أجهزة الصراف الآلي لا توفر بذاتها التأمين

الكافي، لماذا؟ لأنه من الممكن اصطناعها وانتاجها بسهولة، ذلك أن دور البطاقة الممغنطة هو الحماية ضد التخريب العرضي، أما التأمين الحقيقي فيكون في التطابق بين رقم الهوية الشخصي وبين البيانات المشفرة على البطاقة وفي تأمين مسارات الاتصال للرسائل التي تمررها أجهزة الصراف الآلي خلال تشغيلها على الخط مباشرة، أي تأمين عملية الاتصال بين رسالة الطلب ورسالة الرد، أو الاجابة.

انت اذن أمام عناصر ثلاثة هي البطاقة، والبيانات، أو المعلومات، والنظام، لذلك فإن أي عملية تحر، أو تحقيق، أو اشتقاق دليل أو تحليل معملي، أو بحث في بطاقة الائتمانً لابد وأن يتناول هذه العناصر الثلاثة فرادى ومجتمعة، وهذا هو في رأينا المدخل الصحيح لمحاصرة أخطبوط جرائم بطاقة الائتمان.

وإذا كان كذلك، وإذا كانت صور التحايل والتلاعب بالبطاقة من خلال المخاطر الكامنة المصاحبة لعملية الدفع بها، ومراكز الضعف بنظام تشغيلها المذكورة قد صارت واضحة جلية، فدعنا نخطو خطوة أخرى للأمام كي نسأل: كيف يرى خبراء أبحاث التزييف والتزوير جريمة بطاقة الائتمان؟ وما هي أساليب تزييفها وتزويرها؟ ومتى يأتي دور الخبراء؟ توطئة لاشتقاق الدليل العلمي.

الطرق العامة لتزييف بطاقة الائتمان

تتحدد الطرق التي يلجأ إليها المزيف طبقاً لامكاناته وظروفه، والهدف المتوقع تحقيقه، وتعتمد معظم هذه الطرق على الامكانية النسبية لتقليد الشريط الممغنط، أو على امكانية تقليد الحروف النافرة، ويجري تقليد الشريط الممغنط عن طريق محو ما على الشريط الممغنط من بيانات وإعادة

تشفيره ببيانات صحيحة مسروقة، وفي كل هذه الأحوال الثلاث يتضمن الشريط الممغنط المصطنع معلومات صحيحة مأخوذة بطريقة غير صحيحة، كذلك يجري طباعة الحروف والبيانات النافرة أما عن طريق انشائها من عدم أو عن طريق التخلص من البيانات النافرة على بطاقة مسروقة أو انتهت فترة صلاحيتها وذلك بضغطها ثم استحداث بيانات وحروف نافرة جديدة وصحيحة في معظم الأحوال.

وكما هو الحال في جرائم تزييف وتزوير أوراق النقد، وجوازات السفر، وبطاقات الهوية، والشيكات، والوثائق الهامة فإن الصورة الحالية للطرق العامة لتزييف بطاقة الائتمان هو :

١ ـ اصطناع كامل للبطاقة بداية لنهاية، مع النجاح في تقليد أساليب التأمين بها كالصورة المجسمة ثلاثية الأبعاد عن طريق استخدام أجهزة عالية التقنية، فالاصطناع هنا يجري على الجسم البلاستيكي للبطاقة وما عليه من نقوش، وطباعة، وكتابات، وهولوجرام، وشريط ممغنط، وحروف نافرة، وصورة العميل، وشريط التوقيع، وهو ما يطلق عليه الخبراء اصلاح التزييف الكلي.

٢ ـ تزوير البطاقة عن طريق صهر ما عليها من أرقام نافرة لبطاقات مسروقة أو انتهت فترة صلاحيتها، وإعادة قولبتها بأرقام حساب جرى سرقة المعلومات الخاصة بها بطريقة غير مشروعة، أو تقليد الشريط الممغنط عن طريق محو ما عليه من بيانات واعادة تشفيره بمعلومات جديدة وصحيحة ومسروقة، أو إجراء العمليتين معاً، أو كشط شريط التوقيع ووضع آخر مكانه، أو تعرض التوقيع عليه للمحو الآلي أو الكيميائي، أو محو الصورة وطبع أو لصق أخرى مكانها، وفي كل هذا يستثمر المزور الجسم الحقيقي للبطاقة وما عليه من هولوجرام ونقوش،

وطباعة، وكتابة أمنية، وهوما يطلق عليه خبراء الخطوط والمستندات مصطلح التزييف الجزئي.

أساليب التزييف الكلي لبطاقة الائتمان MASS Counterfeit

في قضية جرت أحداثها بين هونج كونج وتايوان، أدى فيها معمل الخطوط والمستندات التايواني دوراً بارزاً، وصدر عنها أول تقرير علمي يعكس الدور المتنامي لخبراء الخطوط والمستندات في عصر الجريمة ذات التقنية العالية (٢٧)، لوحظ أن العصابة الاجرامية قد اتخذت لنفسها مصنعاً لصناعة البلاستيك في منطقة تابعة لمدينة تابي (Taipei)، وبمتابعة أفراد العصابة وجد أنهم بدأوا بشراء التجهيزات المادية اللازمة لانتاج البطاقة، وهي الشريط الممغنط، وأدوات، وآلة تصوير، وآلة طباعة الشبكة النافرة (Embosser)، وآلة لتشفير البيانات على الشريط الممغنط (Encoder)، والة تغليف البطاقة (Laminator)، وقد كان أفراد العصابة يتلقون من متعاونين معهم أسماء حقيقية، وأرقام حقيقية، وشيفرات حقيقية لبطاقات ائتمان حقيقية ومتداولة، حيث يقوم أفراد العصابة بنقل هذه البيانات إلى البطاقات المصطنعة تقليدا لنظائرها الصحيحة، ثم يبيعوا هذه البطاقات المقلدة إلى منظمات اجرامية أخرى لترويجها ولاستخدامها في اليابان، وتايوان، وهونج كونج، وبمبالغ عالية، وفي وكر الجريمة تمكن السلطات التايوانية ضبط عدد (٣٠)بطاقة أميركان أكسبرس و(٩٨١) بطاقة ذهبية، و(١١٥٥) بطاقة داينرز كلوب[٢٧].

هذه هي الصورة المثالية لتزييف بطاقة الائتمان، وإذا رجعنا إلى مخطط المثلث متساوي الأضلاع سوف نجد أنه جرى انتاج البطاقة بتجهيزات مادية متوفرة في الأسواق دون ما ضرورة لوضع ضوابط أمنية على شرائها،

وجرى تلقين البطاقة المصطنعة ببيانات صحيحة مسروقة، وهذا هو الضلع الثاني من المثلث الأمر الذي أدى إلى اختراق النظام عن طريق تداول واستخدام البطاقة، ولا ضرورة هنا لادخال، أو استخدام رقم الهوية الشخصي لأنه لا ضرورة لاستخدام أجهزة الصراف الآلى.

ولو تأملنا قليلاً أنواع البطاقات المصطنعة لوجدنا أنها تخلو من الهلوجرام كما تخلو من الصورة الأمر الذي يقلل من الصعوبات التي تواجه المزيف، كما أنها بطاقات ائتمان، أو بطاقات اعتماد نفقات وهوما يعني أن اكتشاف الجريمة لن يتم قبل مرور شهرين تقريباً من بداية استخدام البطاقات المصطنعة، وتقوم الأهداف الإجرامية هنا على شراء أقصى قدر ممكن من البضائع ثم الاختفاء، أو الهرب لبيعها في مكان آخر والحصول على أموالها.

مشوار اجراء الضبطية هنا طويل والأمل في تحديد الفاعل يبدو ضعيفاً ما لم تتعاون السلطات الأمنية والشرطية، والعدلية عالمياً، وإقليمياً، ومحلياً، فالتوقيع على البطاقة هو توقيع متداولها غير الشرعي، وهو أحد المداخل التي قد تؤدي إلى الفاعل الحقيقي في النهاية، وإذا جرى ضبط أكثر من بطاقة فإن تحديد المصدر مازال ممكنا وذلك عن طريق الوقوف على نوعية اللدائن المستخدمة (البلاستيك)، ومواصفات الحروف النافرة، وأنواع أحبار الطباعة المستخدمة، والعيوب الطباعية للتصاميم والكتابات بالبطاقة، وتحليل المواد اللاصقة، والمواد المكونة للشريط الممغنط، وشريط التوقيع، وإيداع هذا جميعه قاعدة بيانات لاستثمارها في عمليات الربط لتحديد المصدر.

خطوات التزييف الكلي لبطاقة الائتمان عن طريق عمل بطاقة بلاستيكية بداية لنهاية، تبدأ بتقليد الطباعة، والنقوش، والرسوم على بلاسيتك، ثم تغليف البطاقة، ولصق الهولوجرام، والشريط الممغنط، وشريط التوقيع، ثم اصطناع الشريط الممغنط اما بالنسخ، واما بالتشفير، ثم عمل الطباعة النافرة عن طريق انشائها بمعلومات جرى الحصول عليها بطريقة غير شرعية، ثم تداول البطاقة واستخدامها في شراء بضائع، ولكن ماذا لو توفر للمزيف الرقم السري المتوافق مع بطاقة ما؟ عندئذ يمكن للمزيف عمل بطاقة بلاستيكية خالية من أي بيانات، ويوضع عليها شريط ممغنط، ثم تشفير أو استنساخ بيانات صاحب البطاقة، وعمل نسخ عديدة منها، ثم يجري استخدام البطاقة للحصول على أموال من أجهزة الصراف الآلي، ولأن كل الرؤوس الكاتبة / القارئة المستخدمة في أجهزة الصراف الآلي قد جرى تصميمها بحيث تقرأ حتى البطاقات ذات الجودة الضعيفة، فإن تزييفا متوسط الجودة للبطاقة يمكن أن يقبل بسهولة هذه الرؤوس على أنها بطاقة صحيحة، ويطلق على هذه الطريقة في التزييف أحياناً التحايل ببطاقات خالية (White Card Fraud).

هناك صورة أخرى للتزييف الكلي للبطاقة عن طريق سرقة بطاقات كاملة التجهيز المادي من الشركات المنتجة، أو من المصارف بواسطة عملاء بداخل الشركات، أو المصارف، ثم بيعها للعصابات الاجرامية التي تعمل على الحصول على بيانات للبطاقة بطريقة غير شرعية من أحدى المؤسسات المتاحة للمزيف، واستخدام آلات التشفير والطباعة النافرة لتلقين البطاقة بالبيانات المطلوبة ثم تداولها.

ومن الظواهر الدالة على التزييف الكلي للبطاقة نذكر الآتي :

١ ـ عدم دقة لصق وعدم ثبات تموضع الشريط الممغنط وشريط التوقيع بظهر البطاقة الأمر الذي يترتب عليه امكانية نزعها بسهولة بواسطة أظفر الأصبع .

٢ ـ اختلاف مواصفات شكل وحجم البيانات المطبوعة نافرة بالبطاقة المصطنعة عند مقارنتها بنظيرتها الصحيحة ، وفي العادة يستخدم المزيفون آلة طباعة نافرة واحدة لاصطناع البيانات النافرة في البطاقات المزيفة وبغض النظر عن أنواعها والتعدد فيها .

٣ ـ الميل إلى اهمال طلاء الرؤوس البارزة للطباعة النافرة .

٤ ـ الميل إلى اهمال تقليد الهولوجرام ، وإذا جرى تقليده فإن هذا التقليد في معظم الأحيان يكون ردئياً يخلو من الخواص البصرية المميزة للهولوجرام الصحيح ، وفي الأصل النموذجي الصحيح لتموضع الهولوجرام بالبطاقات الصحيحة الحاملة له يجب أن يتخلله الأعداد الأربعة الأخيرة من رقم البطاقة ، وهو ما قد يفشل المزيف في عمل الضوابط الآلية اللازمة لذلك .

٥ ـ امكانية عدم التطابق بين البيانات المشفرة على الشريط الممغنط وبين البيانات المقروءة بصريا والمطبوعة طباعة نافرة .

٦ ـ عند فحص البطاقة وما عليها من نقوش وكتابات ، وشعارات ، ورسوم مطبوعة يلاحظ خلوها مما تتسم به نظيرتها الصحيحة من دقة ووضوح ، وانتظام ، وتناسق ، وحيوية ، ويشوبها التقطعات ، والتشوهات الطباعية .

٧ ـ خلو البطاقة المصطنعة من الخواص المميزة للطباعة المجهرية ، ونتيجة

للنقص في الامكانيات التحليلية لآلات التصوير التجارية التي يستخدمها المزيفون، فإن تقليد الطباعة المجهرية يواجه بعقبات تقنية يترتب عليها اتسام مواضع الطباعة المجهرية بالتشوه أو بالتقطع أو بالتكسر.

٨ـ اهمال العلاقات الترابطية المميزة لاصدار البطاقة الصحيحة، أو الفشل في تقليدها بمواصفاتها، وخواصها المميزة.

٩ـ خلو البطاقة المصطنعة من التأمينات غير المرئية، والسرية المميزة لنظيرتها الصحيحة والتي تنجز بالاحبار الفورية غير المرئية.

أساليب التزييف الجزئي لبطاقة الائتمان (Forged Credit Card)

يستثمر المزيف هنا الجسم الحقيقي للبطاقة وما عليه من هولوجرام، ونقوش، وطباعة، وكتابة أمنية، ثم يقوم بتزوير البطاقة عن طريق صهر ما عليها من أرقام نافرة لبطاقة مسروقة، أو انتهت فترة صلاحيتها، وإعادة قولبتها بأرقام حساب جرى سرقة المعلومات الخاصة بها بطريقة غير مشروعة، أو تقليد الشريط الممغنط عن طريق محو ما عليه من بيانات وإعادة تشفيره بمعلومات جديدة، وصحيحة، ومسروقة، أو اجراء العمليتين معاً، أو الكشط المادي لشريط التوقيع ووضع آخر مصطنع مكانه، أو المحو الآلي، أو الكيميائي لشريط التوقيع، أو محو الصورة وطبع أو لصق، أوحفر أخرى مكانها.

من صور التزييف الجزئي للبطاقة هو الحصول على بطاقة ائتمان صحيحة مسروقة، أو إنتهت فترة صلاحيتها، ثم التخلص من البيانات المطبوعة طباعة نافرة عن طريق تسخينها بواسطة التسخين في الماء لدرجة الغليان وضغط الحروف النافرة حتى تختفي، ثم عمل أرقام وبيانات جديدة

مطبوعة طباعة نافرة بواسطة آلة طباعة نافرة، وتشفير البيانات اللازمة على الشريط الممغنط بواسطة جهاز تشفير بعد محو ما عليه من بيانات قديمة، أو الاكتفاء باحدى العمليتين فقط.

صورة أخرى من صور التزييف الجزئي هو الحصول على بطاقة ائتمان صحيحة مسروقة، ثم كشط ما عليها من شريط توقيع ولصق آخر مكانه، والتوقيع عليه بتوقيع يستطيع المزيف كتابته بطلاقة، أو الابقاء على الشريط ثم تقليد التوقيع الصحيح على البطاقة المسروقة عند امضاء فواتير الشراء، أو المحو الآلي، أو الكيميائي للتوقيع الأصلي أو لأجزاء من هذا التوقيع إذا كانت البطاقة المسروقة مزودة بصورة العميل، قد يلجأ المزور إلى التخلص من الصورة، أو تغطيتها ووضع صورة أخرى في موضعها أما بالحفر، أو باللصق، أو بالحفر واللصق معاً.

ومن أهم الظواهر الدالة على التزييف الجزئي بالبطاقة نذكر الآتي :

١ ـ انهيار بعض مواضع من شريط التوقيع وامكانية ظهور سطح البطاقة أسفل مواضع الانهيار نتيجة للمحو الآلي.

٢ ـ ظهور بقع قاتمة، أو بنية، أو مصفرة اللون، أو انقشاع الأنساق الطباعية لأرضية شريط التوقيع كاشفة عن فجوة تبدو على هيئة جزيرة لا تتواصل فيها خطوط وألوان وكتابات هذه الأنساق الطباعية نتيجة للمحو الكيميائي.

٣ ـ إذا كان شريط التوقيع قد تعرض للكشط المادي، ثم جرى لصق شريط آخر مصطنع في مكانه، فإن تموضع الشريط المصطنع يفتقر إلى الدقة والثبات، وقد يترتب على ذلك خدوشات واتساخات تدل على ذلك،

كما قد يترتب على ذلك أيضاً نزيف، أو سيلان للمادة اللاصقة في مواضع حول الشريط المصطنع.

٤ ـ التشوه، أو التقطع في الحافة السفلية للهولوجرام.

٥ ـ وجود تسلخات، أو تهتكات، أو بقع مسودة في المواضع المحيطة النافرة، أو عدم انتظام الرؤوس البارزة للطباعة النافرة.

٦ ـ الاختلاف في مواصفات التشكيل الطباعي لأرقام وحروف الطباعة النافرة عما هو عليه في بطاقة صحيحة مناظرة.

٧ ـ يغلب على البطاقة المزيفة تزييفاً جزئياً اهمال طلاء الرؤوس البارزة لرموز الطباعة النافرة بها.

٨ ـ امكانية عدم التطابق بين البيانات المشفرة على الشريط الممغنط وبين البيانات المقروءة بصريا والمطبوعة طباعة نافرة بالبطاقة.

٩ ـ وجود تقطعات، أو تشوها، أو انبعاجات، أو انخسافات، أو زيادة في السمك، أو رتوش، أو انطماسات بالمساحة التي بها صورة العميل يظهر أو بوجه البطاقة.

١٠ ـ احتمالية عدم التوافق في العلاقات الترابطية التي تنظم وتميز اصدار البطاقة الصحيحة.

هناك طرق أخرى للتحايل ببطاقة الائتمان يمكن اجمالها في النقاط الآتية:

١ ـ تحميل العميل لفواتير مصطنعة.

٢ ـ استغلال خدمات الصراف الآلي في إيداع شيكات بلا رصيد، بحيث تضاف قيمة الشيك إلى قيمة الحساب الأصلية، ثم سحب المبالغ المضافة بواسطة الصراف الآلى قبل اجراء المقاصة بين المصارف.

٣ـ التحايل على أجهزة تحقيق شخصية مزورة للحصول على بطاقات ائتمان صحيحة .

٤ ـ استخدام أوراق تحقيق شخصية مزورة للحصول على بطاقات ائتمان صحيحة .

٥ ـ سرقة بطاقات ائتمان صحيحة ، وسرقة الأرقام السرية الخاصة بأصحابها الحقيقيين من البريد بواسطة موظفي البريد حال ارسالها من المصارف والبنوك إلى العملاء .

٦ ـ التحايل بواسطة الهاتف عن طريق مودم لمعرفة كلمة المرور ، أو مفتاح السر والوصول إلى أرقام بطاقات الائتمان بالمصرف .

٧ـ امكانية اختراق النظام ، وحساب أرقام الهوية الشخصية ، وأرقام البطاقات المناظرة ، وبيانات العملاء واصطناع بطاقات مزيفة تحمل معلومات صحيحة .

٨ ـ قيام الشخص الحامل للبطاقة ، أو آخر حصل عليها بعد انتهاء فترة صلاحيتها ، بكشط ثم تعديل فترة صلاحية البطاقة المطبوعة طباعة نافرة .

المراجع

المراجـــع

(١) توم فويستر، ترجمة محمد كامل عبد العزيز، مجتمع التقنية العالية، مركز الكتب الأردني، ١٩٨٩.

(٢) لن مايرنغ وايان جراهام، ترجمة محمد ابراهيم الطريفي، مدخل إلى ثورة المعلومات، المؤسسة العربية للدراسات والنشر، بيروت، لبنان ١٩٨٩.

(3) Hutcheon, A., Automated teller machine, in computer security reference book, edited by Jackson, K. M., and Hruska, J., Butterworth-Heinemann Ltd., 1992.

(4) Kaine, G. P., Counterfeit credit cards, Interpol conference, Ottawa, 1992.

(٥) ألفن توفلر، ترجمة ل. ر. ، المعرفة : صناعة الرموز، مجلة القاهرة، نوفمبر ١٩٩٣، ص ص ٦٦-٧٢.

(6) No author, Credit cards clinging on, the economist, Vol. 329, No. 7838, Nov. 20, 1993, pp. 78-79.

(٧) رياض فتح الله بصلة، العملة البلاستيكية : جريمة العصر القادم، الندوة العربية لتأمين العمليات المصرفية ضد التزييف والتزوير، المركز القومي للبحوث الاجتماعية والجنائية، القاهرة، مصر، أكتوبر ١٩٩٤، ص. ١-٢٥.

(8) Holland, K., Stalking the credit-card scamsters, business week, Jan. 17, 1994, pp. 4041.

(9) D' Amelio, J. R., Overview of worldwide credit cards fraud, Interpol Conference, Ottawa, Canada, 1992, pp. 1-6.

(10) Sharif, R. M., Credit where credit is due, Gulf Marketing Review. Vol. 1, Oct. 1993, pp. 22-24.

(١١) سرقات بواسطة بطاقات الائتمان في الأردن، جريدة العرب، العدد ٦٤٠٠ ، ١٥ يونيو ١٩٩٤م.

(١٢) زكريا، خضر، ظاهرة تزييف بطاقات الائتمان تغزو الدول العربية، جريدة الشرق الاوسط، ملحق اقتصادي، العدد ٣٧ ، ٣١ يوليو ١٩٩٤م، الدوحة، قطر.

(١٣) نادية سلطان، تزوير بطاقات الائتمان، جريدة الخليج، العدد ٥٦٠٢ ، ١٥ سبتمبر ١٩٩٤ ، الشارقة، الامارات العربية المتحدة.

(١٤) أنيس ديوب، الجرائم الاقتصادية قيد السيطرة، الشرق، العدد ١٤٧ ، ٣٠/ ١ـ٥/ ٢ سنة ١٩٩٥م.

(15) Swanson, C.C., Chamelin, N. C., and Territo, L., Criminal investigation, Fifth edition, MC Graw-Hill, Inc., New York, U.S.A., 1992, pp. 446-451.

(16) Adler, F., Mueller, G.O., and Laufer, W. S., Criminalogy, MC Graw-Hill, INC., New York, U.S.A., p. 271.

(١٧) محمد صالح عثمان، تزوير المستندات وتزييف العملات والأساليب العلمية للكشف عنهما، المنظمة العربية للدفاع الاجتماعي ضد الجريمة، القاهرة، مصر ١٩٧٨ .

(١٨) أحمد السيد الشريف، الحديث في التزوير والتزييف، دار المعارف، القاهرة، مصر ١٩٧٢م.

(١٩) رياض فتح الله بصلة، مقدمة في طرق تزييف العملة الورقية وأساليب التعرف عليها للعاملين في البنوك وهيئة البريد، معهد علوم الأدلة الجنائية، القاهرة، مصر، ١٩٨٥، ص ص ٣ـ ٤ .

(٢٠) معوض عبد التواب، الوسيط في شرح جرائم التزوير، والتزييف، وتقليد الأختام، منشأة المعارف، الاسكندرية، مصر ١٩٨٨ .

(21) Spencer, R. L., and Giles, A., Multiple-Processing of visa vochers, J. for Sc. Soc., Vol. 26, 1986, P. (401).

(22) Davis, D., Schemes for Electronic Funds Transfer at the point of Sale, in Computer Security Reference Book, Edited by Jackson, M.K., and Hruska, J., Butter Worth-Heinemann Ltd., 1992.

(23) Uehling, M.D., Taping the code, Popular Science, Oct. 1993, P. (46).

(24) Schneier, B., Digital Signatures, Byte, Nov. 1993, PP. (309-312).

(25) Hellman, M.E., The Mathematics of Public-Key Cryptography, Scientific American, Aug. 1979, PP. (130-139).

(26) Uehling, M.D., Crackling the Uncrackable Code, Popular Science, Sept. 1994, P. (43).

(27) LIU, J.K., and Chang, R.W., Investigation and Examination of Credit Cards Forgery: A Case Report, Presented at the 45th Annual Meeting of American Academy of Forensic Sciences, February 15-20, Boston, MA, USA.